Stay Open. OX

WHITE PAPER | VERSION 1.0

DNS-over-HTTPS
and the Rise of OTT DNS

Table of Contents

1. Executive Summary

Known as “the phonebook of the internet,” the Domain Name System (DNS) is a vital part of the infrastructure that gives users an optimized internet experience. As such, DNS forms a critical control point on the web.

The recently released DNS over HTTPS (DoH) protocol allows DNS queries to be encrypted and transmitted over the internet as encrypted HTTPS traffic. Encrypted DNS provides end-user data privacy and secures one of the last remaining unencrypted internet protocols. This new DNS encryption capability is fuelling the trend toward “over-the-top” (OTT) DNS and significantly altering how DNS is used and networks perform.

Over-the-top DNS can have considerable consequences for network operators who often use their DNS servers to direct customers to the correct (regional) CDN, block malware, phishing, and botnet activities, and enforce government mandates and regulatory blocklists. If network operators cannot manage DNS services, they lose an important control point over their network traffic.

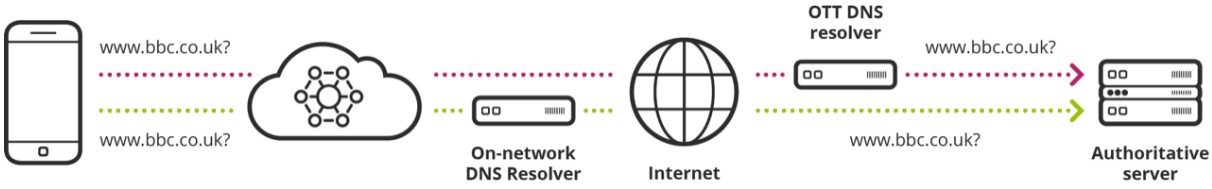
This whitepaper describes the importance of DNS for operators, examines the trend of moving DNS to third party providers, and discusses how network operators can offer similar privacy enhancing features and stay in the game.

2. DNS as the Address Book of the Internet

Introduction

A key element in the process that provides access to internet services, DNS acts as the address book of the internet by providing human-readable domain names for internet services. Almost without exception, every action on the internet, from visiting a website, using a service via a mobile app (e.g. a messenger app), or checking and sending emails, starts when the client such as the browser, app, or email-client, looks up the IP address of the service by using the domain name system.

It is only after the IP address of the service is ascertained that further communication between a client and the service can continue and the relevant IP packets are routed over the internet. Since all online activities start with a DNS lookup, it is clear fast and highly reliable DNS service is vital for a positive customer experience.



3. Importance of DNS for operators

Traditionally, internet service providers included local, robust DNS resolution to customers as part of their fixed or mobile network connection. In this chapter we explain the reasons why DNS is important for operators and their subscribers.

DNS Performance & Latency

Since every connection on the internet starts with a DNS request, a slow DNS response influences end-users' quality of experience (QoE). "If the DNS is slow, the internet feels slow."

Modern web services require multiple DNS requests, so it follows, DNS is more important than ever. Although every action on the web starts with a single request, most web pages and services these days load content from multiple locations, which requires additional DNS queries. If every query is answered slowly, additional time quickly adds up and adversely impacts the user's experience.

In many ways, an internet subscriber's online experience depends on fast and reliable DNS infrastructure. Although internet service providers usually market their "download speeds" in advertisements, fast domain name resolution is at least as important to the user experience. For example, Ofcom specifically measures and compares DNS-resolution times for UK providers when they benchmark broadband providers in their periodic "UK Home Broadband Performance" reports[1].

Content Delivery Based on Location

As bandwidth use continues to increase approximately 30% a year and more people switch from television to streaming services, the demands on networks grow.

In order to optimally route traffic and prevent data from being unnecessarily transported over large distances, operators and Content Delivery Networks (CDNs) often work together to place CDN-nodes for content, streaming, and other services at locations in the operator's network that are geographically closer to the end-user. Localized CDNs allow users to connect to a server that is located near them. This reduces latency and ultimately increases performance. Location-based content delivery allows network operators to make optimal use of the regional network capacity and reduces backhaul across their core network, and this reduces costs.

Locating the right server for a user is accomplished in various ways, but usually DNS is used. Operators share the location of specific (IP) subnet ranges on the CDN and/or the streaming provider and the user's IP address, included with every query (often using 'edns client-subnet'[2]), is added. This way, the content provider can calculate the approximate location of the user and reply with the IP address of the closest server.

It is vital for network providers to control their DNS and work closely with CDNs to provide content from the best server. Operators can then provide high performance, low latency connections, and meet their customer's streaming or internet of things (IoT) needs.

[1] https://www.ofcom.org.uk/research-and-data/telecoms-research/broadband-research/home-broadband-performance-2017
[2] see https://tools.ietf.org/html/rfc7871

Detection of Malicious Activities

Many Internet service providers use DNS to protect end-users. Providers can block specific domains to stop malware, phishing-links, and botnets based on threat intelligence.

In addition to blocking malicious domains based on threat intelligence, (near)real-time analysis of DNS traffic also provides valuable insights into how and where malware or botnets propagate on the provider's network. DNS analysis has become a valuable tool for network providers' security and anti-abuse departments.

It is even more important to offer network-based DNS protection against IoT-based botnets because of the enormous increase in IoT devices. Already cameras, routers, and even baby monitors have been hacked. When these devices are infected with malware and then used as botnets, they can create a virtual army of DoS devices. With the diversity of operating systems and firmware, DNS-based network protection is a good way to contain the risk.

Providers also use DNS to provide protection through parental control services which block (per household or per device) specific content that has been deemed inappropriate. This service uses DNS domain categorization so parents control what their children are allowed to access.

Government Regulation and Court Order Compliance

DNS also plays an essential role in helping service providers comply with government regulations and local court orders. Operators often use DNS blocklists to forbid access, such as when they want to block illegal file-sharing or terrorist websites.

4. Trends: Moving to OTT Encrypted DNS

There are three trends currently changing the way DNS functions. The combination of these trends could lead to further centralization of the internet, less choice for consumers, and reduced control for operators over their network, all of which harm network performance.

Encryption and Privacy

Over the last few years, there has been a concerted effort to encrypt much of the traffic on the internet, and today, most websites have migrated to HTTPS. DNS remained one of the few non-encrypted internet protocols. To address these data privacy concerns within the DNS framework, the Internet Engineering Task Force (IETF) introduced two new DNS standards:

- DNS over TLS (DoT) – Encryption over a raw TLS-encrypted channel.
- DNS over HTTPS (DoH) – Encryption over an HTTPS channel.

Both standards address user privacy requirements by offering different ways to encrypt DNS queries and responses while in transit. Some device operating systems and browsers already use those standards. The Android 9.0 (Pie) attempts to connect via DoT by default before falling back to the unencrypted DNS service, and Firefox currently offers DoH support.

Per-Application DNS settings

Applications traditionally used the DNS settings as configured by the network provider's DHCP service for the operating system.

DoH has been a catalyst for applications, particularly web browsers, to do their own DNS resolution, independent of the network/operating system settings.

When browsers or other applications perform DNS queries directly, each can choose its name server, different from that used by other applications and from the one configured in the operating system.

Moving to OTT DNS

Although it has always been possible to use a third-party DNS service, the name resolution landscape has changed significantly in recent years with the appearance of a number of over-the-top DNS providers. Google started its 8.8.8.8 service in 2010 and has been joined by additional DNS providers such as Cloudflare (1.1.1.1), QuadNine (9.9.9.9), and others. These cloud-based DNS providers offer high-speed resolution and secure surfing to end-users.

With multiple cloud DNS providers to choose from, Mozilla plans to move all Firefox users' DNS requests to one of a trusted set of DoH-supporting resolvers which support strict privacy requirements known as Trusted Recursive Resolvers, or TRRs[3]. Trusted Recursive Resolvers must support DoH-compliant DNS services and commit to strict user privacy for DNS queries.

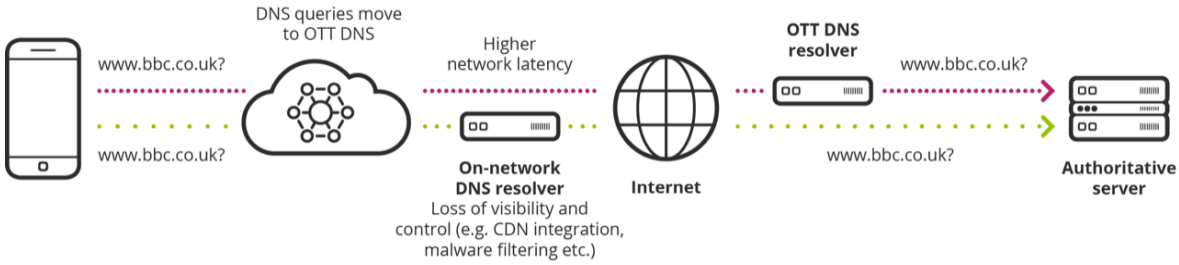
Google will also support DoH in their Chrome web browser, which has almost 65% market share[4]. However, their approach is different from Mozilla:

- Chrome will attempt to contact a DoH resolver as provided by the local network.
- If a DoH server cannot be contacted, Chrome will fall back to unencrypted DNS.
- Chrome will provide options for users to configure a different OTT DoH-compliant resolver similar to Mozilla.

[3] https://wiki.mozilla.org/Security/DOH-resolver-policy
[4] https://en.m.wikipedia.org/wiki/Usage_share_of_web_browsers

Consequences

Although the trend to add encryption to DNS traffic should be encouraged as part of data privacy reforms, there are significant concerns for network providers and their customers. Specifically, the end-user internet experience will be further concentrated among a handful of companies, service providers will lose a key network control point, regulatory restrictions will be difficult to enforce, and the user QoE may suffer.



Privacy for the End-user?

Cloud-based DNS providers argue that offering DNS over HTTPS enhances end-user data privacy. Although the data is encrypted and difficult to view or capture directly, network providers already have access to their subscribers' traffic as it traverses the provider's infrastructure. By pushing the DNS traffic to OTT DNS providers instead of the network provider, yet another party has access to the end-user data. In areas like the EU with strict privacy regulations such as GDPR, moving the DNS to an external resolver may not improve privacy at all. Remember, the DNS provider sees all user browsing and other internet activity, which is considered very private information.

Control over the Network

As we described, DNS is used to direct internet traffic and can improve the user experience by the coordinated use of DNS with CDNs. When content providers install content services (i.e. video streaming) within the network's infrastructure, DNS is the primary tool used to connect end-users to the co-located content. Content providers, network operators, and users all benefit from the close integration of DNS and CDNs.

If DNS resolution moves to an OTT provider, the network operator loses this level of traffic control. Even in a best-case scenario, network providers must backhaul traffic across their entire network and peering links to content servers located outside their network. This leads to increased costs for the operator and worse user experience.

Parental Control, Malware and Phishing protection

DNS is an important part of an operator's malware and phishing prevention service. When DNS moves to a third party, operators lose a valuable tool to implement government regulations and court-ordered blacklists. Third-party DNS resolution also eliminates high-value services that providers could offer like parental control and malware protection.

End-users, however, might still contact the operator when malicious activity affects their service. A bad DNS service is thus likely to provoke calls to the network provider's help desk even though they won't be able to provide additional protection or analyse the problem.

Without control over DNS, network providers lose a number of security features and processes. Local governments, however, still hold the operator responsible for protecting users, offering secure internet access, and complying with local regulations and court orders.

End-user Experience

Many of the cloud DNS providers argue they provide faster DNS management services. We have found this is often not true, and local DNS services are, or at least can be, faster than cloud services. This is no surprise; networks gain several milliseconds of latency advantage when the DNS is close to users as opposed to third-party services located elsewhere.

However, not all operators have raised their DNS to the highest standards. In those cases, the cloud-based DNS resolution might actually be faster. We strongly suggest all operators carefully monitor their DNS and ensure their DNS-service is configured to the highest standards. Once subscribers move their DNS to the cloud it is a major challenge to win them back.

5. What Should Operators Do?

Top-notch DNS management services are important for network operators, content providers, and users. A quality end-user experience relies on low latency and high-speed DNS responses that reside in the same jurisdiction. In the interest of data privacy, providers should support the latest standards for encryption and privacy, including DoT and DoH, and use Domain Name System Security Extensions (DNSSEC) to enforce resolution.

Operators need to act fast or they will lose a critical control point for managing their network traffic. If they surrender this control, providers won't be able to block malware, botnets, and phishing, and will de facto be dependent on third party, over-the-top providers to deliver their customers' entire internet experience.

Based on current developments and trends, network operators can take the following actions:

1. It is vital that network operators adopt these security and privacy enhancements quickly and provide encrypted DNS. They can achieve this by implementing DoT and DoH on their current DNS infrastructure, and continue to offer legacy unencrypted DNS. In this way, any application that prefers DoT/DoH can discover and use the local encrypted resolvers.

2. Operators must ensure their DNS is as fast as possible. This means the operator's DNS server must be optimally configured to provide the most stable and low latency DNS responses feasible. The goal is to make sure end-users have the best DNS experience from their local operator and not from an OTT provider. Operators have an advantage; they own the final hop to the customer device. In this way, as browsers and other software start to discover and prefer encrypted services, operators can maintain their preferred position.
3. Finally, operators should ensure they support the latest standards, such as client-subnet, to provide locality information to CDN partners, and make sure users have a superior overall experience compared to OTT DNS providers.

6. PowerDNS for a Fast, Private DNS solution

About PowerDNS

PowerDNS was founded in 1999 and has been a leading open-source provider of DNS software since 2001. With headquarters in the Netherlands, PowerDNS is part of the Open-Xchange (OX) Group of companies, which are dedicated to keeping the internet open, safe, and free.

PowerDNS is designed specifically for large-scale DNS service providers, including mobile and fixed-line broadband operators, hosting, and cloud service providers.

PowerDNS Recursor and DNSdist

Unlike other DNS resolvers, PowerDNS provides an extremely powerful caching resolver and a unique DNS proxy and load-balancer called DNSdist. Deployed together, they provide an unrivalled set of features for DNS service.

A modern, high-performance DNS cache resolver, PowerDNS Recursor offers:
- Highly multi-threaded resolution, optimizes usage on modern, multi-core hardware
- Extremely low and predictable latency for records delivered from the cache
- DNSSEC validation
- Lua policy engine for ultimate customizability and flexibility
- Malware and content filtering engine (including parental controls)
- Mobile app for end-user alerting and reporting framework
- Query logging and reporting DB

A uniquely powerful DNS proxy, DNSdist offers:
- DNS-aware load balancing using a variety of balancing and high availability techniques
- Rich Lua-based policy engine
- DDoS protection
- DNS tunnelling and exfiltration detection
- DNS over TLS and DNS over HTTPS support
- DNS query packet caching
- Policy-based query routing

DNSdist is unique because it works when it is placed in front of any DNS resolver, including legacy lookup tools.

PowerDNS Performance and Latency

Latency is a key metric for optimal DNS, and thus overall network performance. In a real-world deployment, a PowerDNS resolver service that handled millions of queries per second answered 90% of all queries in 2ms or less and answered 99% in less than 5ms. The remaining queries were for cache-misses and thus required a DNS lookup to an authoritative server.

PowerDNS Caching and CDN Support

PowerDNS Recursor combined with DNSdist provides extremely advanced caching capabilities, for example:

- Load balance DNS queries to resolver pools based on arbitrary information in the DNS packet, including query name, query type, source IP address, etc., in order to optimise cache hits or to shared cached queries by resolver.
- Tiered caching – for example using a small cache (including caching client-subnet responses from CDNs) in Edge DNS servers and forwarding queries to a pool of servers with a large cache which are configured to not cache client subnet responses. Tiered caching provides an optimal balance between fast localized DNS responses and minimal latency for domains that are looked up less frequently.

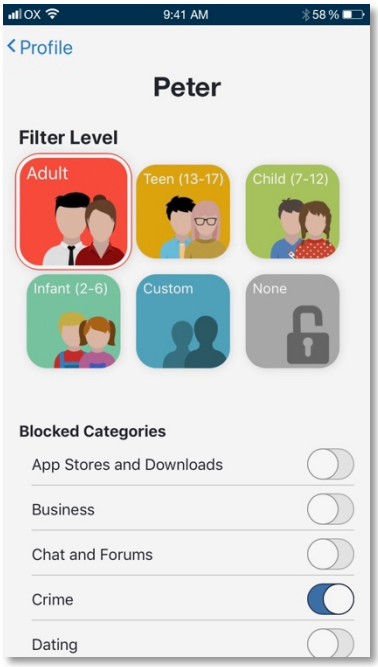
Support for CDNs is twofold:

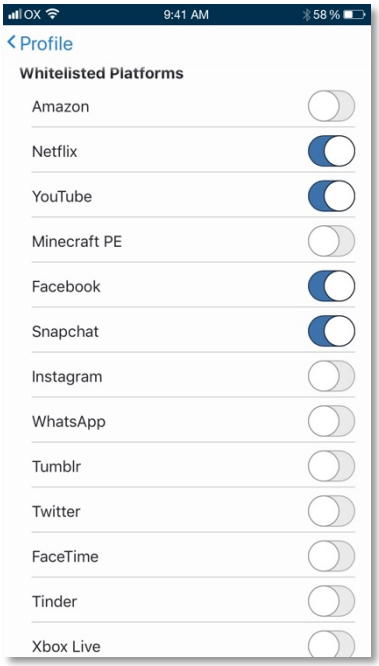
1. EDNS client-subnet support to pass information about the original IP address to the downstream server. This is supported in both Recursor and DNSdist. The client-subnet-specific information returned by the CDN can be cached or not, depending on the configuration and requirements. Caching is performed on a per-subnet basis to ensure the integrity of answers specific to each subnet.
2. Locality tagging in an Edge DNS deployment – when the locality is known a specific client-subnet can be configured for all requests from a recursor. This allows caching to be performed in the same manner for all requests, which means a much higher cache hit rate.

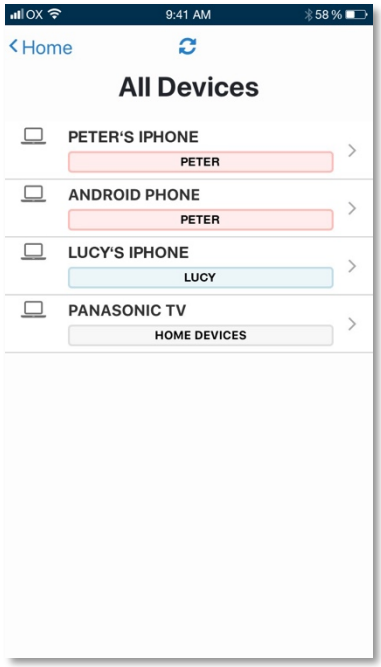
PowerDNS Filtering

PowerDNS Recursor comes with extremely powerful malware and content-filtering controls, including:

- System-wide or per-user malware filtering, including phishing, malware, and botnet command-and-control as separate categories.
- System-wide or per-user content filtering based on an internet categorization feed. This can be used to implement network-based parental controls or enterprise content filtering.
- Malware and content categorization feeds can be optionally bundled, and custom or third-party feeds easily integrated.
- Alert/notification support via SMS, email, push notifications to end-users, or webhooks to operators.
- End-user facing REST-APIs, including OAUTH support, to build mobile apps that control settings and receive notifications.







7. PowerDNS Security and Privacy

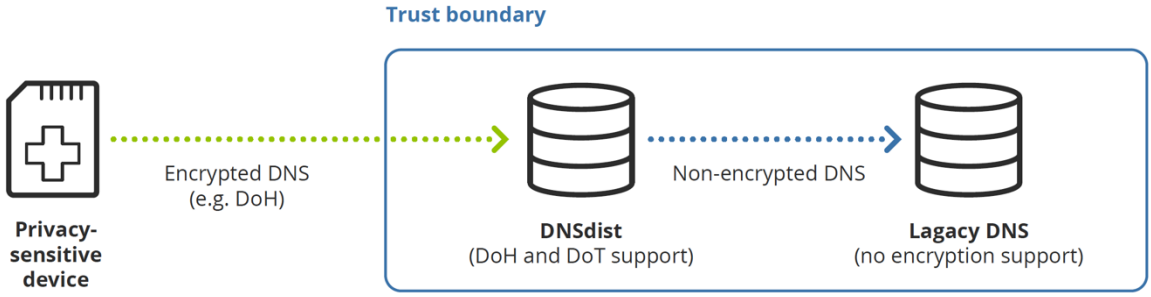
PowerDNS supports the latest standards in encryption and privacy:

- DNS over HTTPS (DoH) – encrypts DNS queries between devices and the resolver
- DNS over TLS (DoT) – encrypts DNS queries between devices and the resolver
- DNSSEC – validates DNSSEC protected records for enhanced integrity of DNS responses.

The following features are on the Roadmap:

- Qname minimization – prevents leaks of extraneous query information to authoritative servers.
- DNS over TLS – encrypts DNS queries between the resolver and the authoritative server.

DoT and DoH support are part of DNSdist, which means DNSdist can be used to add encryption support to legacy DNS services, as shown in the following figure:



PowerDNS to Provide Encryption to Your Legacy DNS

DNSdist is a uniquely powerful DNS proxy that offers a variety of features, including DNS over TLS and DNS over HTTPS. Since DNSdist can be placed in front of any DNS resolver, including legacy resolvers, operators can get all the benefits of its features by simply adding DNSdist to a legacy DNS infrastructure.

Summary

DNS as the “phonebook of the internet” is a vital part of the infrastructure required to provide an optimal internet experience. As such, it is an important control point on the internet.

The recently released DNS over HTTPS (DoH) protocol that allows DNS to be encrypted and sent over the internet disguised as HTTPS traffic, combined with cloud-based DNS providers, will significantly alter the way DNS is used.

Encrypted DNS alone is an improvement. It provides additional data privacy and gives users flexibility. However, the combination of DNS encryption and the fact that some players on the internet have started to use a select set of so-called trusted DNS services now threatens the open nature of the internet.

Already, Mozilla and Google offer support for DoH in their browsers and DoT on Android. Both organizations have announced they will give preference to encrypted DNS over unencrypted DNS in the near future.

This trend has significant consequences for network operators who use their DNS servers to route traffic to the correct regional CDN, block malware, phishing, and botnet activities, and enforce government blocklists. If end-user DNS resolution is no longer under their control, network operators lose a key way to manage traffic. Since DNS resolution is fundamental to the end-user network experience, the perceived quality of the network could be heavily influenced by third-party DNS systems. Customers and end-users are unlikely to understand the difference and potentially will blame the network operator for third-party DNS delays, outages, or security issues.

There are a number of immediate actions that will mitigate the risk of losing network control.

- Most importantly, providers must take the lead and implement the technology that enables DoH and DoT services on their DNS servers so they can provide the very latest privacy features to their customers.
- Operators must ensure their DNS servers are optimally configured and provide the most stable and low latency DNS responses possible. Network operators must make sure end-users get the best DNS QoE possible from them and not from a cloud-based server which is usually a couple of milliseconds away.
- Providers can differentiate themselves by offering value-added DNS services such as malware protection, parental controls, and key event notifications to their customers.

Please reach out to Open-Xchange if you have any questions or requests. We are happy to support and help you implement encrypted DNS and further improve your DNS solutions.